Taller de Administración de Servidores Linux

CC5308

Clase 32: 31 de mayo de 2011

Alta Disponibilidad

Luis León Cárdenas Graide
lcardena [at] nic . cl

High Availability (HA)

- Disponibilidad: Posibilidad de comunidad de usuarios para
  - Acceder al sistema
  - Trabajar en el sistema: crear, actualizar, alterar
  - Consumir trabajo del sistema
- Indisponibilidad / Downtime
- BCP: Protocolo de Diseño e Implementación
- SLA: ¿Para qué (objetivos)?
  - Garantías, multas, contratos
  - Cuantificable: Medición => **Monitoreo**

Niveles de Disponibilidad

- Cuántos "nueves"
  - 90% ~52K min/año ~36 día/año
  - 99% ~5K min/año ~3,6 día/año
  - 99,9% ~520 min/año
  - 99,99% ~52 min/año (¿años bisiestos?)
  - 99,999% ~5 min/año (!)
  - ... e intermedios
- 100% Disponibilidad = Costo Infinito (infactible)
  - "Ilusión" de continuidad
  - FUD marketero y publicidad engañosa
    - (100% Seguridad, Riesgo cero)

Cuánta Disponibilidad

- Recuperación: MTBF y MTTR
  - Eventualmente infinito (¡considerarlo!)
  - Programado vs Inesperado (SLA)
  - Total vs Parcial (SLA)
- Disponibilidad = MTBF / (MTBF + MTTR)
- Disminución Downtime vs Aumento Complejidad
  - Disponibilidad más difícil de evaluar
  - Cambios en SPoF's: Eventual empeoramiento
    - Reevaluar
- Uptime: Faceta Seguridad (tradeoff costo-beneficio)
- No reinventar la rueda: Patrones de Diseño HA

Disponible para/según quién

- Múltiples vistas: Extremos vs Intermedios
  - Administrador de Sistemas
  - Cliente Interno/Externo
  - Intermediarios
  - Proveedor
- SLA: Múltiples monitoreos
  - Monitores "neutrales" y "comprehensive"
  - Ojo con overhead
- Estimación MTBF y MTTR: según fuente monitoreo
  - Experiencia propia histórica / ajena publicada
- Definición Operacional

Planificación Downtime

- Scheduled: Lógico (usualmente)
  - Update, Upgrade, Reboot, Seguridad, Middleware
- Unscheduled: Físico (usualmente)
  - Hardware, Energía
  - Lógico: Caídas SO/Aplicaciones
- Impacto downtime: BCP
  - Peaks horarios: transacciones vs volumen ventas

Diseño HA

- ¿Requerimientos HA? SLA
- Patching software
  - Hotpatching (SO)
- Escalabilidad Incremental
- Redundancia
  - Pasiva vs Activa
  - N-m: N-1
- Testing: Stress vía remoción de componentes
  - ¡Hasta que falle!
  - Medir

Causas de Falla Top

- Carencia de "mejores prácticas"
  - Control de Cambios
  - Monitoreo de componentes relevantes
  - Requerimientos y Aprovisionamiento
  - Operaciones
  - Evitar "fallos de red"
  - Evitar fallos internos en aplicaciones
  - Evitar falla de servicios externos
  - Ambiente físico
  - Redundancia de red
  - Solución de respaldo técnico
  - Solución de respaldo de procesos
  - Ubicación física
  - Redundancia de infraestructura
  - Arquitectura de redundancia de almacenamiento

Cluster HA

- High Availability (HA) != High Performance (HP)
  - Diseño: Uno, otro, ninguno o ambos
- Cluster HA Infraestructura
  - Failover: Entra nodo que toma control otro caído
  - Failback: Retoma control nodo original al volver
- Cluster HA Aplicación
  - Migración de datos y aplicaciones
  - Redundancia
- Monitoreo mutuo de nodos en cluster
  - Monitor central (SPoF) vs varios (cluster) monitores
  - Split-brain: Sub-clusters incomunicados. Corrupción

Actividad Personal

- Linux HA: Heartbeat http://www.linux-ha.org
- Xen: MV{1,2}+eth{0,1}, br{0,1}
  - MV1: eth0+IP10-br0, eth1+IP11-br1
  - MV2: eth0+IP20-br0, eth1+IP21-br1
  - dom0: br1
  - Heartbeat MV1-MV2 por br0
  - ping de dom0 a IP11
  - Crash MV1
  - Failover: MV2 responde por eth1 como IP11
  - Failback: MV2 cede a MV1 y vuelve a IP21